National Infrastructure Protection Center CyberNotes

Issue #9-99 *April 28, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 10 and April 24, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold.**

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[1] **(Updated vulnerability data)[2]**	**ColdFusion Application Server**	**Machines loaded with the Expression Evaluator (sample application) will allow authorized individuals to read and delete files on the server.** ***Unauthorized web users can upload files (possibly including executable files) to the server.***	**Remove all sample applications and code from production servers and obtain patch for Expression Evaluator at: http://www.allaire.com**	**ColdFusion Expression Evaluator unauthorized access**	**High**	**Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit. Other related hacker tools can be utilized to gain privileged access.**

[1] Allaire Security Bulletin, ASB99-01.
[2] L0pht Security Advisory, April 20, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BMC Software[3]	PATROL management software	It is possible to replay the session password enabling an unauthorized user to gain a root shell	No workarounds or patches known at time of publishing.	PATROL session replay	**High**	Bug discussed in newsgroups and Web sites.
BMC Software[4]	PATROL management software	A Denial-of-Service attack is possible using UDP.	No workarounds or patches known at time of publishing.	PATROL UDP Denial-of-Service	Low	Bug discussed in newsgroups and Web sites.
CISCO[5]	Cisco router (Running version 12.x to 12.0(4)X)	If NAT and the input access list are on the same router interface it is possible for packets to be "leaked." A user could then circumvent security filters/policies without knowing the fact.	Patches and full details of IOS's effected can be obtained at: http://www.cisco.com/warp/public/770/iosnatacl-pub.shtml	CISCO NAT problem	Low/ Medium	Bug discussed in newsgroups and Web sites.
eBay	System problem	A malicious user can use JavaScript embedded in HTML to obtain another user's username and password. With this, the malicious user can retract bids, change password and conduct other operations.	No official patch known at time of publishing.	eBayla	Medium/ **High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Flowpoint Router	aSDL routers	Many companies ship their routers with no password or easily guessed passwords.	User should change passwords upon receiving the router.	Default passwords	**High**	The use of default password(s) continues to be the number one exploitable vulnerability.
HP - UX[6] (HP3000)	Operating System (MPE/iX debug)	User can gain increase privileges due to improper handling of commands by debug.	Patches now available from Hewlett-Packard (HP). For: MPE/ix 5.0 - MPEKXM1A MPE/ix 5.5 - MPEKXM1B	HP-UX MPE/iX debug problem	Medium/ **High**	No activity on this vulnerability found.
HP - UX[7] HP9000 series 700/800	Operating System (Sendmail)	Users can create a Denial-of-Service condition.	Patches available: HP-UX 10.20 - PHNE_17135 HP-UX 11.00 - PHNE_12190	HP-UX Sendmail DoS	Low	Bug discussed in newsgroups and Web sites.
Internet Security Systems, Inc.[8] (ISS)	Internet Scanner (IS) (version prior to 5.6.3)	When checking for IP Spoofing, some check may run against random addresses. Some of these addresses may not be associated with the user of IS.	ISS has made available version 5.6.3 at: http://www.iss.net	IIS Internet Scanner out of range check	**High**	Bug discussed in newsgroups and Web sites. Originator may be identified as an intruder on other systems.
Microsoft	Internet Explorer (IE) V 5.0	Web site owner is notified when an end user adds the web site to "Favorites."	No official patch known at time of publishing.	IE 5.0 favorites problem	Low	Bug discussed in newsgroups and Web sites.

[3] BUGTRAQ, April 9, 1999.
[4] BUGTRAQ, April 9, 1999.
[5] CISCO web site.
[6] Hewlett-Packard Daily Security Bulletin Digest, April 13, 1999.
[7] Hewlett-Packard Daily Security Bulletin Digest, April 20, 1999.
[8] ISSforum, April 12, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft	Internet Explorer (IE) V 5.0	Conducting a web search for a specific file "favicon.ico" will reveal sites that may expose CGI scripts, including passwords, to viewing.	No official patch known at time of publishing.	IE 5.0 favorites problem	**High**	Bug discussed in newsgroups and Web sites. This problem may also assist hacker in identifying mis-configured sites.
Microsoft[9] (Vendor patch update)	Internet Explorer (IE) V 5.0	A hostile web site owner may be able to determine information about a visiting computer through "IMG SRC" tags. A hostile web site owner may be able to execute a Java Scriplet on the visiting computer with trusted privileges. A hostile web site owner may be able to paste contents into the visiting computer clipboard.	Patches available at: http://www.microsoft.com/windows/ie/security/mshtml.asp	IE 5.0 MSHTML problem	Medium	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Microsoft[10]	Internet Explorer 5.0	Vulnerability in the DHTML edit control allows a remote site to obtain and/or read files on the local machine. Note that this is similar to the "%01 security bug" discovered in January.	Patches available at: http://www.microsoft.com/windows/ie/security/dhtml_edit.asp	IE 5.0 reading and sending of files (a.k.a. %01 bug again, DHTML edit)	Medium/ **High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Microsoft[11] Windows 95/98	Operating system	When a machine receives multiple ARP requests it may result in the user of that machine having to click "OK" for each request, effectively causing a Denial-of-Service condition.	No official patch known at time of publishing.	Windows ARP Denial-of-Service	Low	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Mirabilis[12]	ICQ99a (build 1700 v2.13)	Telnetting to Port 80 and sending "Quit <LF>" will cause the webserver to crash. This bug appears to be intermittent.	No workarounds or patches known at time of publishing.	ICQ web server crash	Low	Bug discussed in newsgroups and Web sites.

[9] Microsoft Security Bulletin MS99-012, April 21, 1999.
[10] NTBUGTRAQ, March 30, 1999.
[11] BUGTRAQ, April 12, 1999.
[12] BUGTRAQ, April 8, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Novell NetWare[13] (V 4.1X) (Note that this attack was first discovered in August 1998.)	Pandora V 3	An attacker can spoof NCP calls over the IPX protocol. This will enable the attacker to grant Supervisor rights to a guest account or to create a Denial-of-Service condition	Vendor recommends: Install support pack 5B and set the server signature level to 3 (the highest level) and the client packet signature to 1 (1 is the default setting for both). Note that several people have indicated that setting NCP packet signature to Level 3 will prevent Microsoft's client for Netware from logging in[14].	Pandora Hack	Medium/ **High**	Bug discussed in newsgroups and Web sites.
RealNetworks [15] Inc.	Real Media Server	The program stores the password in cleartext. On Linux machines it is store with a 644 permission setting and on NT machines it is stored with file permissions set to full access for everyone.	No official patch known at time of publishing.	Real Media Server password access problem	Medium/ **High**	Bug discussed in newsgroups and Web sites.
Sun Microsystems	JAVA JDK 1.1 and Java 2	A suspected flaw in the "byte code verifer" will allow code that has not been checked to run. This may enable an attacker to gain full control of the system by running the attacker's code.	Patch available at: http://java.sun.com	JAVA 2 sandbox problem (a.k.a. Byte code verifer)	Medium	Bug discussed in newsgroups and Web sites.
Unix – Digital Unix[16] 4.0 (*prior to 4.0E*[17]) **Update to versions affected**	**Operating System (inc)**	**Buffer overflow condition exists in the /usr/bin/mh/inc file. This condition can allow an unauthorized user to gain root access.**	**No workarounds or patches known at time of publishing.**	**Digital Unix inc buffer overflow**	**High**	**Exploit Script now available. Explanation of exploit available in newsgroups.**

[13] Novell Technical Information, 2941119, last modified April 9, 1999.
[14] BUGTRAQ, April 13, 1999.
[15] BUGTRAQ, April 14, 1999.
[16] BUGTRAQ, January 25, 1999.
[17] Compaq Software Security Team Advisory, April 6, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix – Digital Unix[18] 4.0 *prior to 4.0E*[19] **Update to versions affected**	**Operating System (at)**	**Buffer overflow condition exists in the "at" program that can allow an unauthorized user to gain root access.**	**Upgrade to Digital Unix 4.0D or obtain appropriate patch at: ftp://ftp.service.digital.com/public/dunix**	**Digital Unix at buffer overflow**	**High**	**Exploit Script now available. Explanation of exploit available in newsgroups.**
Unix[20] - NetBSD	Operating System	Unprivileged users can cause a file-system locking error. This occurs during certain kernel operations when a path name ends with a symbolic link ending with one or more "/".	Patch for NetBSD 1.3.3 is available at: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/19990412-vfs_lookup	NetBSD symbolic link kernel panic	Medium	Bug discussed in newsgroups and Web sites.
Unix - NetBSD[21]	Operating System (shell script "SVR4_MAKEDEV")	An unprivileged user can read and write data on the first IDE disk.	Patch is available at: ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/19990419-SVR4_MAKEDEV	SVR4_MAKEDEV script vulnerability	**High**	Explanation of exploit available in newsgroups.
Webcom[22] (not Webcom.com)	CGI Guestbook	An unauthorized individual may read any text file if the path to file is known. On NT machines, Anonymous Internet Accounts must have read access, but on Windows 95/98 all text files are readable.	No workarounds or patches known at time of publishing.	Webcom's CGI Guestbook	Medium	Explanation of exploit available in newsgroups.
Winroute[23]	Winroute Pro 3.04	Unauthorized user can gain access to software configuration without authentication.	No official patch known at time of publishing.	Winroute Pro configuration access	**Medium**	Bug discussed in newsgroups and Web sites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

(continued on next page)

[18] BUGTRAQ, January 25, 1999.
[19] Compaq Software Security Team Advisory, April 6, 1999.
[20] NetBSD Security Advisory 1999-008, April 13, 1999.
[21] NetBSD Security Advisory 1999-009, April 19, 1999.
[22] NTBUGTRAQ, April 9, 1999.
[23] BUGTRAQ, April 9, 1999.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between April 10 and April 24, 1999, listed by date of script, script name, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 35 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
April 23, 1999	**Coldscan.c**	**A scanner that checks for Cold Fusion Application Server vulnerabilities.**	
April 23, 1999	Cgiv3.c	A CGI scanner that checks for 43 different vulnerabilities.	
April 23, 1999	**Httptunnel-2.3.tar.gz**	**Allows a user to tunnel through a restrictive firewall that has an HTTP proxy.**	
April 23, 1999	ICQ.webserver.txt	Detailed instructions of how to execute a number of attacks against ICQ99a Webservers.	
April 22, 1999	**Nessus-alpha2-fix4.tgz**	**Network security auditing tool that checks for 208 vulnerabilities, detects remote services, portscans and more. This version fixes a number of segmentation faults and increases performance.**	
April 21, 1999	Ipps-1.0.tgz	Port scanner	
April 21, 1999	mc-kill.c	Exploit that allows local user to obtain root on a machine running Midnight Commander 4.XX.	
April 21, 1999	**Mole.cfm**	**Cold Fusion template that allows remote attacker full access to files on a Cold Fusion application server.**	
April 21, 1999	Shopping Cart	Exploit description for use against most commercial and freeware shopping carts.	
April 20, 1999	Mars	Java application the monitors SMTP, POP3, HTTP, and FTP.	
April 18, 1999	**Httpdtype-0.07.tar.gz**	**Program that attempts to identify the type of web server running on a remote host.**	
April 18, 1999	KKI.dos	Denial-of-Service script against several RPC implementations.	
April 17, 1999	**Abelkiller.zip**	**Program that removes both the Cain and Able programs.**	
April 17, 1999	Nessus-alpha2-fix3.tgz	See entry for April 22, 1999.	
April 16, 1999	**Abel v1.1**	**Trojan horse that accesses user passwords on Microsoft Windows 9X machine. It can be used in conjunction with the "Cain" tool.**	
April 16, 1999	**Cain v1.51**	**Password cracker/recovery tool for use on Microsoft Windows 95/98 systems.**	
April 16, 1999	Nmap/nlog tool set	Collection of scripts and utilities that enhance nmap and/or nlog.	
April 16, 1999	Snort v0.99rc6	Packet logger.	
April 16, 1999	Snort-0.99rc6-lib	Sample rule set for Snort.	
April 15, 1999	Mac	Exploit script for a buffer overflow in the Responder.cgi script for MacHTTP.	
April 15, 1999	Miffo-check-1.4.tar.gz	Port scanner that scans class B or Class C IP ranges.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
April 15, 1999	**Nwrap**	**Nmap add-on that will randomize host/port scanning combination in an effort to remain stealthy.**	
April 15, 1999	Scr1.41.zip	Source code for a Windows version of Back Orifice client.	
April 14, 1999	**Cgichk1.3c**	**Program that checks for 41 Common Gateway Interface (CGI) vulnerabilities and, if any are found, will attempt to exploit the most common.**	
April 14, 1999	Tcpflow-0.11.tar.gz	Program that captures data transmitted as part of TCP connections. This program will reconstruct packet in sequence.	
April 12, 1999	Exdump-0.2.tar.gz	Packet logger that can monitor content and direct output to a user-defined file.	
April 12, 1999	**Sdi-wu.c**	**Exploit script that creates a backdoor on systems with the WU-ftpd long directory names vulnerability. This program also includes a worm that will scan for other vulnerable systems and attempt to exploit those systems.**	
April 11, 1999	Hunt-1.3.tgz	Connection hijacking tool.	
April 11, 1999	Netbsd.symlink	Code that causes a file-system locking error on NetBSD systems. This results in a system panic or hang.	
April 11, 1999	NT-BSOD.c	Denial-of-Service code against Microsoft Windows NT. Exploits the Windows NT PE loader vulnerability resulting in "Blue Screen of Death."	
April 11, 1999	**Poink.c**	**Denial-of-Service code against Microsoft Windows 95/98/NT. Exploits handling of ARP packets.**	
April 10, 1999	Explpine.c	Exploit code that allows local user to elevate privileges.	
April 10, 1999	Netscape.4.5.passwd .c	Exploit code that retrieves passwords from Netscape 4.5 ~user/.netscape/liprefs.js files and decrypts the passwords.	
April 10, 1999	Ratc.c	UNIX/Linux source code for the RAT Trojan horse.	
April 10, 1999	Remote.zip	Remote Novell NLM password decrypting program.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period:

1. Large numbers of scans and attacks continue to be directed at machines running the Linux or Sun Solaris operating systems.
2. Viruses continue to be written to capture and transmit information or spam other Internet sites.
3. Large numbers of SMTP servers are being scanned for common user names, most likely in an effort to obtain names for spam attacks.[24]
4. Probes to port 1800 and 1945 have been observed recently.
5. Probes continue to look for machines with Back Orifice installed.

Viruses

A list of the top ten viruses infecting two or more sites as reported to various anti-virus vendors has been categorized into the two tables below. The first table list macro viruses, and the second table lists other viruses. Macro viruses have, historically, spread fastest due to their ability to be transferred by e-mail.

For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite), trends (based on number of infections during the last three months reported), and approximate date first found.

Note: Virus reporting is normally 6 to 8 weeks behind the first discovery of infection. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages, as soon as updates become available.

The viruses listed in the virus table infected over 84,000 machines in March/April, which represents an increase in the number of reported infections from the last prevalence table. When the Melissa virus is removed from the count, the number of reported infections for the March/April timeframe continues to indicate an increase in viruses discovered over the last reporting period. The number 1 ranked virus (Melissa) for March/April accounted for 81,000 reported infections, and the last virus listed in the tables infected 11. A total of 493 distinct viruses were reported this month, infecting over 3,000 sites. **Infection rates are based on number of machines infected, not number of sites**. This method reflects the way statistics are being gathered and reported by a number of anti-virus vendors.

Table 1 – Macro viruses:

Ranking	Common Virus Name	Type of Virus	Date First Reported
1	Melissa	Macro	March 1999
2	ColdApe	Macro	December 1998
3	Class	Macro	September 1998
4	Laroux	Macro	July 1997
5	Ethan	Macro	February 1999
6	CAP	Macro	April 1997
7	Npad	Macro	December 1996
8	Concept	Macro	December 1996
9	Temple	Macro	December 1998
10	Marker	Macro	February 1999

[24] A number of states have enacted legislation making spamming illegal.

Table 2 – Other viruses:

Ranking	Common Virus Name	Type of Virus	Date First Reported
1	W95/CIH	File	July 1998
2	AntiEXE	Boot	September 1994
3	AntiCMOS	Boot	October 1995
4	Form	Boot	September 1991
5	Junkie	Multi	July 1994
6	Empire.Monkey	Boot	July 1994
7	Parity_Boot	Boot	September 1993
8	Sampo	Boot	January 1995
9	Stoned	Boot	September 1994
10	DelCMOS.B	Boot	January 1999

Virus shipped out with newsletter - An Internet freeware/shareware software distribution newsletter has indicated that the program "TimePiece 1.0" may contain a virus. Anyone who downloaded this software before April 20, 1999 should obtain a new copy of this program.